MUCO

Moravian Business College Olomouc

Security of Terminal Equipments

Lukáš Pavlík, Ph.D.
Department of Informatics and Applied Mathematics
E-mail: lukas.pavlik@mvso.cz

Security Concept, Security Policy, Security Measures

- Information technology brings a number of current issues to the information security program.

- In addition, the rapid development of information technology has a major impact on the effectiveness of the implemented security program.

- Most of the issues raised are based on the important fact - that technology alone will not solve these requirements and problems, and existing security measures may be ineffective with new information technologies.

Security Concept, Security Policy, Security Measures

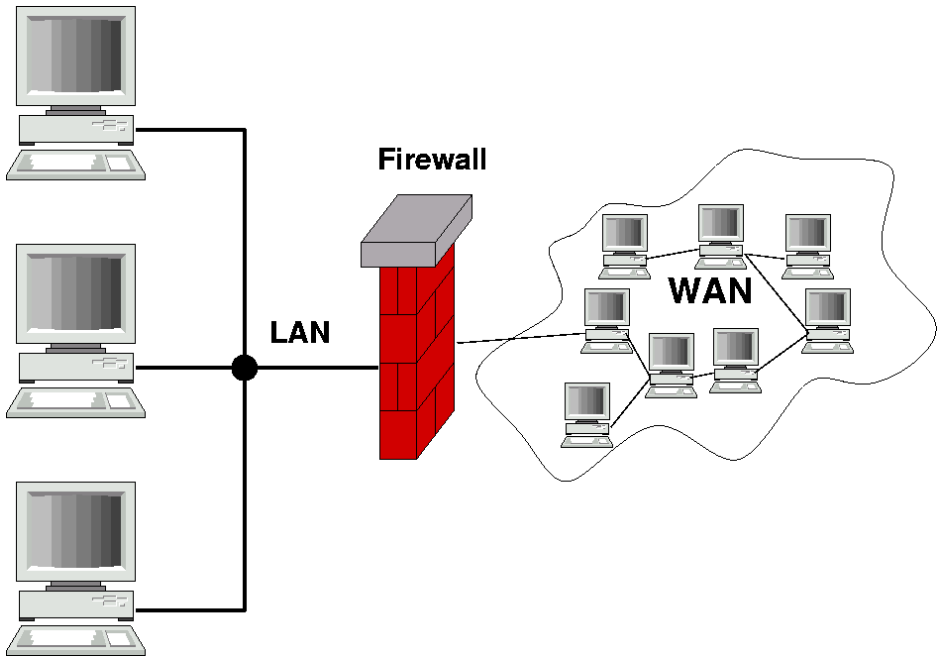
- On the other hand, when overestimating the possibilities of technologies (declared in the safety parameters of a given product), it is easy to make the wrong decision, which often puts the company in a situation where it has to look for measures against unnecessary risks.

From the system point of view, there is a need to address the following requirements at the technology level:

- authentication, authorization, administration of user accounts;
- VPN;
- antivirus protection;
- risk management;

Security Concept, Security Policy, Security Measures

- firewall;
- system intrusion detection management;
- data content filtering;
- encryption.



Firewalls

- Firewalls form an "electronic" circuit around an enterprise computing environment.
- Firewalls have filters that allow you to bring only certain types of network communication to the company's network and prevent access to any other data that does not meet the criteria of security, authenticity, etc.
- In this way, firewalls create a basic security pass on access to the enterprise information system.

Firewalls

- When designing the deployment of firewalls in an enterprise environment, a trade-off between speed and security must be considered.

Firewalls can be categorized as follows:

- packet filtering by firewalls;
- status firewalls;
- protection methods at the application layer or proxy server.

Firewalls

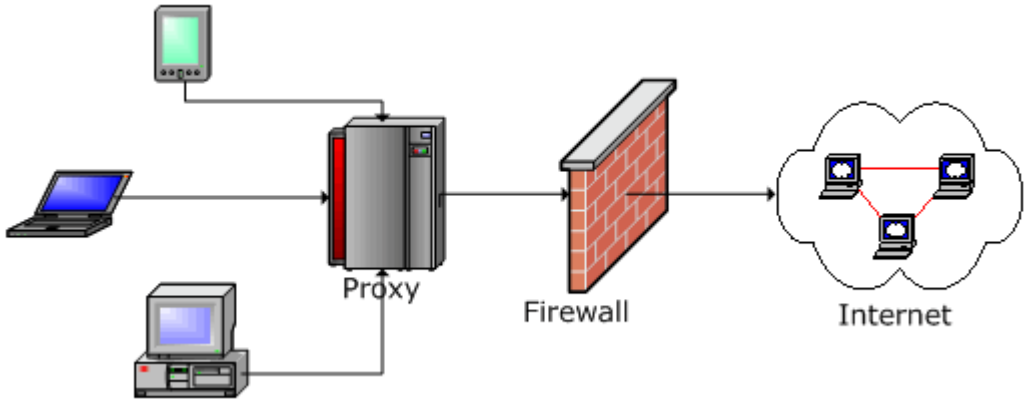
- Protection methods in firewalls using packet filtering verify the headers, resp. address, packet, or message information to identify potential problems, based on the rules set, either the incoming packet is blocked or released.
- Stateful firewalls monitor the status of a transaction to verify that the destination of an incoming packet matches the source and the previous outgoing request.
- The firewall checks the connection of incoming packets against previous outgoing packets to determine their legitimacy.
- The firewall uses correlation with the state connection table and, unlike a packet firewall, examines the context of data packets, i.e. the source and destination addresses of the message, rather than filtering them.

Firewalls

- The most secure firewalls are application layer firewalls or proxy server firewalls.
- The firewall analyzes the content of incoming packets according to the results of the analysis and decides whether only valid messages will be released to the network.
- This is the safest way to filter because it is difficult to write inappropriate content to the data portion of packets.
- The disadvantage is that this process significantly reduces the permeability.
- There are several variants of these firewall solutions, where a packet firewall is preceded by the application firewall to be a load on the application firewall, which only processes filtered packets.

Firewalls

- The representative of application firewalls is a proxy firewall, here all data always passes through a proxy server, which filters them according to the set conditions.
- The advantage of this type of application firewall is that the user's source addresses are hidden, as the application gateway is listed behind it.



Antivirus Software

- As with humans, it is essential to protect against viruses in the electronic environment.
- Antivirus software helps prevent computers from being infected with malicious software (computer viruses, worms, trojan horses, etc.).
- Collectively, it can be defined as malware protection.
- As hundreds of new types of malicious software are added every day, it is necessary and mandatory to update antivirus software regularly with new virus definitions.

Antivirus Software

- In addition, attacks have become much more sophisticated over the years, and nowadays it is much easier for malware to infect your computers than in the past, as new malicious software exploits several different system vulnerabilities at the same time and creates new forms for its spread.

- These threats have led the security industry to develop tools that regularly automatically select virus definitions, often once a day, to prevent infections quickly and effectively.

- When malicious code infects your computer, security vendors offer tools that remove infections from your computer and try to clean up any damage caused by a virus.

Antivirus Software

- Antivirus software is a required part of an information security program due to the growing number of viruses.
- Only with implemented antivirus software (recommended by several manufacturers) it is possible to proceed to the safe use of the Internet.
- Anti-virus software must provide comprehensive protection against all types of threats in the Internet environment.
- That's why security software vendors deliver "packages" of antivirus software that cover a known spectrum of malicious software.

Vulnerability Management

- Vulnerability management is a way to proactively address vulnerabilities in an information security program.

- An effective security program uses tools to automatically manage vulnerabilities to identify potential vulnerabilities in an enterprise information system.

- Vulnerability management tools compare the environment with a database of known vulnerabilities and check which vulnerabilities the enterprise information environment contains.

Vulnerability Management

- There are two types of vulnerability management tools: network and host.
- You can use network-based tools to scan network communications for known vulnerabilities and host tools for scanning physical devices, such as computer servers.
- Due to the growing number of vulnerabilities, it is necessary to ensure the current patching of information programs.
- This is a complex task because patches must be tested before they can be applied, which in the case of large enterprises with a large information environment (a large number of applications, servers and users) requires a systematic approach that must be integrated into the business processes.

Vulnerability Management

- A regular and controlled program for scanning information environment vulnerabilities and a system for dealing with necessary repairs must be part of ensuring an adequate level of security for the business.

- For this reason, SIEM is integrated into the information environment.

- Error management technology is therefore an important part of an information security management system.

- These tools allow you to proactively identify vulnerabilities and take the necessary proactive security measures.

IDS – Intrusion Detection System

- Intrusion Detection Systems (IDS) monitor traffic and events on the network and in enterprise information systems, where they detect signs of a possible attack, or information about attacks that have been carried out.

- As with vulnerability management, intrusion detection tools can be provided in two modes, i.e. in a network or host environment.

- Network-based tools actively seek out traffic on key parts of your network and look for possible attacks.

IDS – Intrusion Detection System

- Host tools run on servers and check audit or log information to detect possible attacks.
- Because data log evaluation can be resource intensive, these tools can adversely affect server performance.
- In this case, it is necessary to continuously monitor the "throughput" of the information system, but when reducing it, it is not possible to solve the situation by disabling the tools that detect intrusions.
- These tools rely on two methods of intrusion identification: description-based recognition and anomaly detection.

IDS – Intrusion Detection System

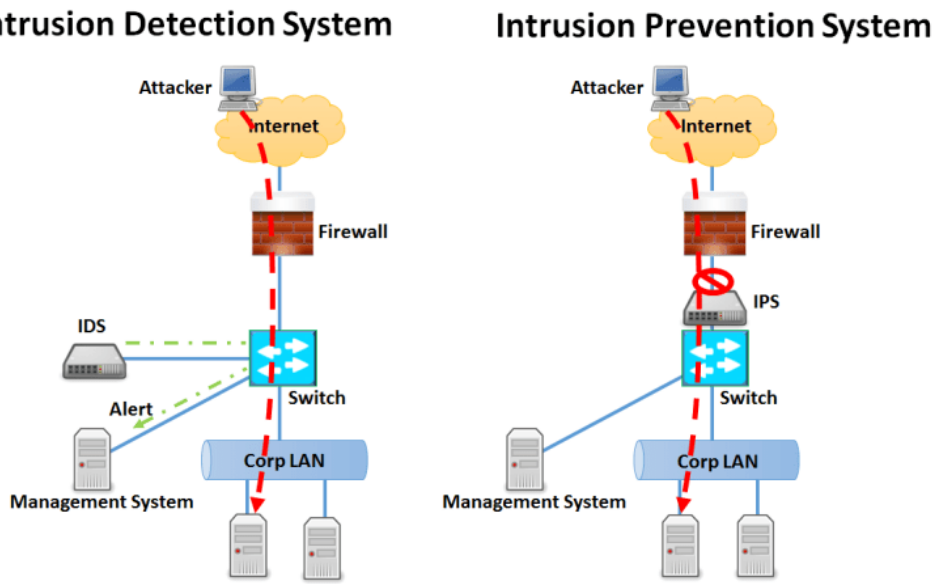
- Description-based recognition compares certain patterns of activity with unknown attack scenarios.
- Description-based intrusion detection tools detect patterns or signs of abnormal activity.
- Here, the detection of a non-standard situation depends on the identification of samples for normal behavior and then on the detection of behavior that differs from the standard.
- Both of these methods must respond to a high degree of variability in the controlled environment and determine what the standard situations are and what the attacker can dispose of.

IPS – Intrusion Prevention System

- Typical corporate networks are connected to several external networks. R
- emote branches can be connected to the central network using various technologies (fixed lines, DSL, various types of VPN…), thus creating a large network.
- Due to the variety of possible attacks, it is not possible to solve the security perimeter of the company only using firewalls, but it is necessary to design security zones, which structure security tools with separation into individual areas - Internet, DMZ (demilitarized zone, Intranet, etc.).
- Rules for data transfer must be set, while the basic rules are set on the firewall.
- Intrusion detection and prevention systems (IDS / IPS systems) are intended for the transmission and control of critical data.

IPS – Intrusion Prevention System

- IPS systems, as well as IDS systems, are divided into network and host.
- Both categories have in common the monitoring of the system, the ability to notify the administrator of a possible attack and make a security r



IPS – Intrusion Prevention System

- Host systems are deployed directly to individual stations or servers.
- These are software products and are therefore limited by OS support on the station.
- They monitor system calls, logs and the like.
- Protects against attacks on OS and applications.
- Network systems are specialized devices for monitoring network events.

IPS – Intrusion Prevention System

- The Intrusion Prevention System (IPS) is able to detect and respond to attacks at the same time (i.e. to prevent or interrupt an attack).

There are 2 types of monitoring set here:

- attack on malicious software applications;
- Internet attack - DoS, DDoS attacks.

Comparison of IPS and IDS

- IPS, thanks to the ability to prepare a response to attacks, provide a more reliable way of protection.
- However, this reaction can also have a negative impact.
- These are so-called false alarms.
- In connection with this, it can disconnect an authorized user or completely block network traffic on a given network segment.

IPS – Intrusion Prevention System

- Some IDS systems can also respond to an attack by working with a firewall that dynamically changes its policy to prevent attacked traffic.

- Intrusion detection and prevention systems are implemented as specialized devices that are managed from a central control system.

Enforcement of Security Measures at the Application Level

- Security issues arise whenever unauthorized persons gain access to data sources or when users exceed the level of access to the systems defined by them.

- Within Information Technologies, methods for controlling access to information and communication systems can be used to regulate user access so that they behave in accordance with their needs and in defined areas.

- It is important that in the implementation of the security program, security measures for this issue are aligned with the value of protected information.

BYOD, IoT Control and Monitoring

- Currently, there is a significant problem with the security of so-called endpoints.
- Business computing infrastructure is often secure, but its weaknesses are burners, printers, USB media, users' laptops and smartphones.
- Weak points are also "smart" products, where the reason for their deployment is the automation of routine activities, whether in households (refrigerators, washing machines, heating), but in the corporate structure, controlled by remote access via the Internet, which brings new security threats.
- This is a new phenomenon of IoT (Internet of Things)
- And last but not least, the rapidly expanding BYOD, ie the use of the user's device in the corporate network, while no corporate "image" is installed in this device.

Safety of Industrial Systems (SCADA, PLC)

- Data obtained from safety data monitoring sensors must be processed or prepared for inspection by a designated operator.

- The data from the sensors can be displayed when captured in their format, i.e. in a table as a sequence of measurements with a time stamp.

- However, data in such a form are difficult for the responsible person to interpret, therefore these data are converted into a simpler form before their display, enabling their visualization.

Safety of Industrial Systems (SCADA, PLC)

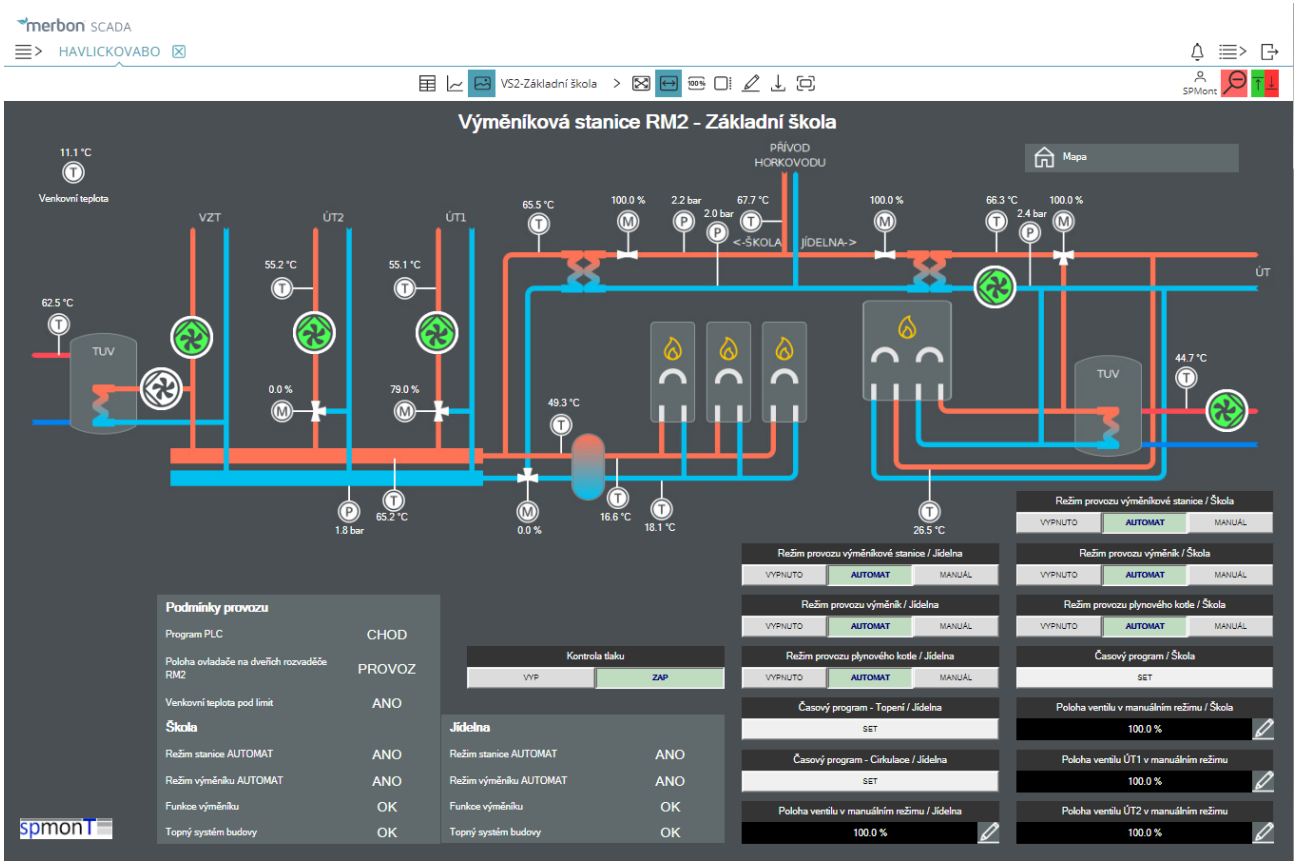
- The so-called SCADA (Supervisory Control and Data Acquisition) systems are used for this purpose.

- SCADA systems form another layer in the logic of industrial automation. The lowest layer consists of PLC automats regulating the process in real time.

- The SCADA system, because it has to, read (usually over the network), process and display the data, works in "almost" real time.

- It is important to realize that the SCADA system does not obtain information directly from sensors (via PLC), but from a defined location, especially from a powerful database server.

Safety of Industrial Systems (SCADA, PLC)



Safety of Industrial Systems (SCADA, PLC)

- These servers are referred to as real-time databases. It is also possible to consider a direct connection between SCADA and PLC, but it is necessary to consider that the PLC is adapted to the regulation, but is not able to provide information in a form comparable to a relational database.

- However, the advantage is that it is easy to set the PLC to use a database server as a data storage (PLC-database connection) and to connect this server to the SCADA system (database - SCADA).

Thank you for your attention